

10

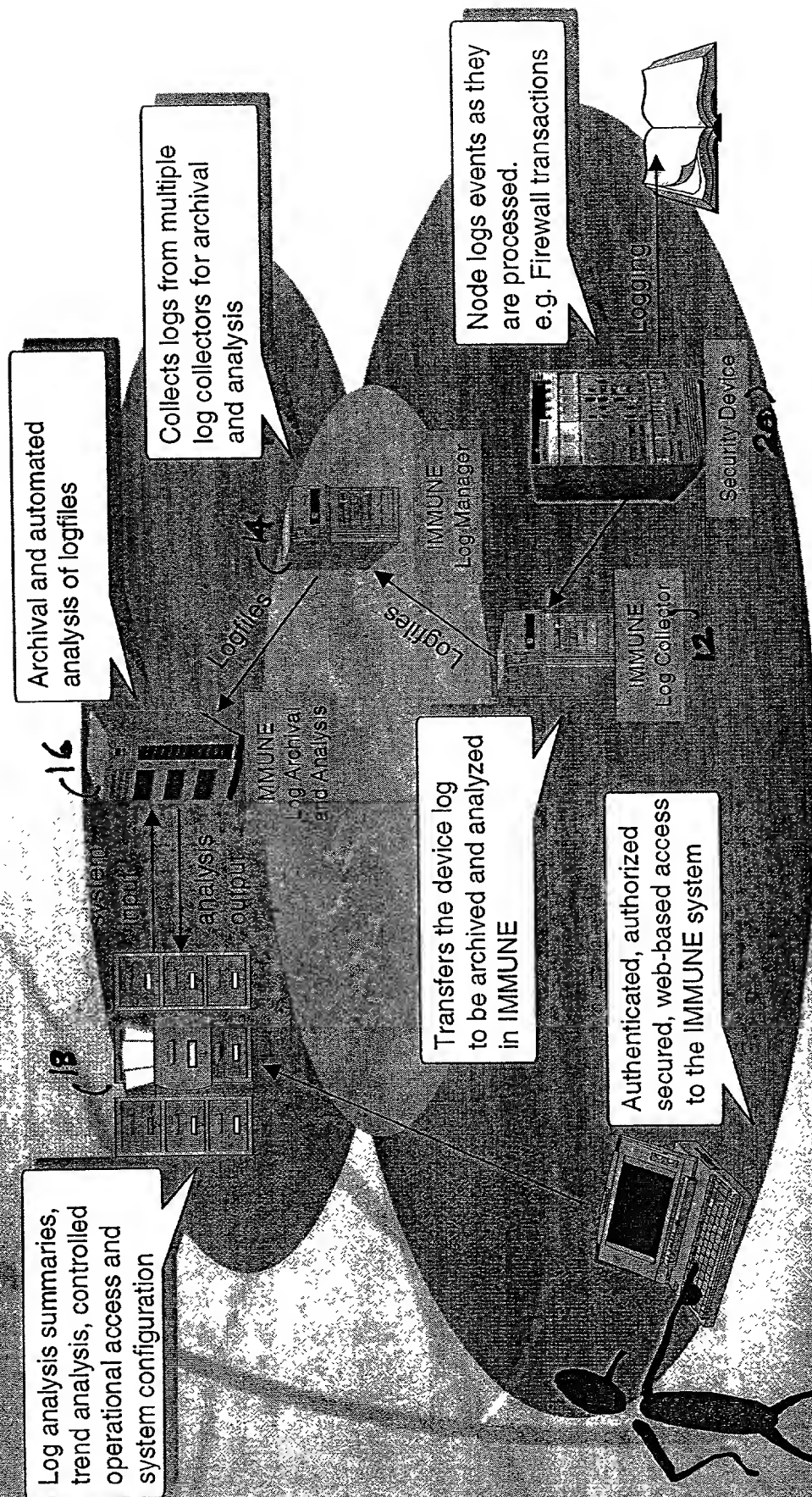


FIGURE 1

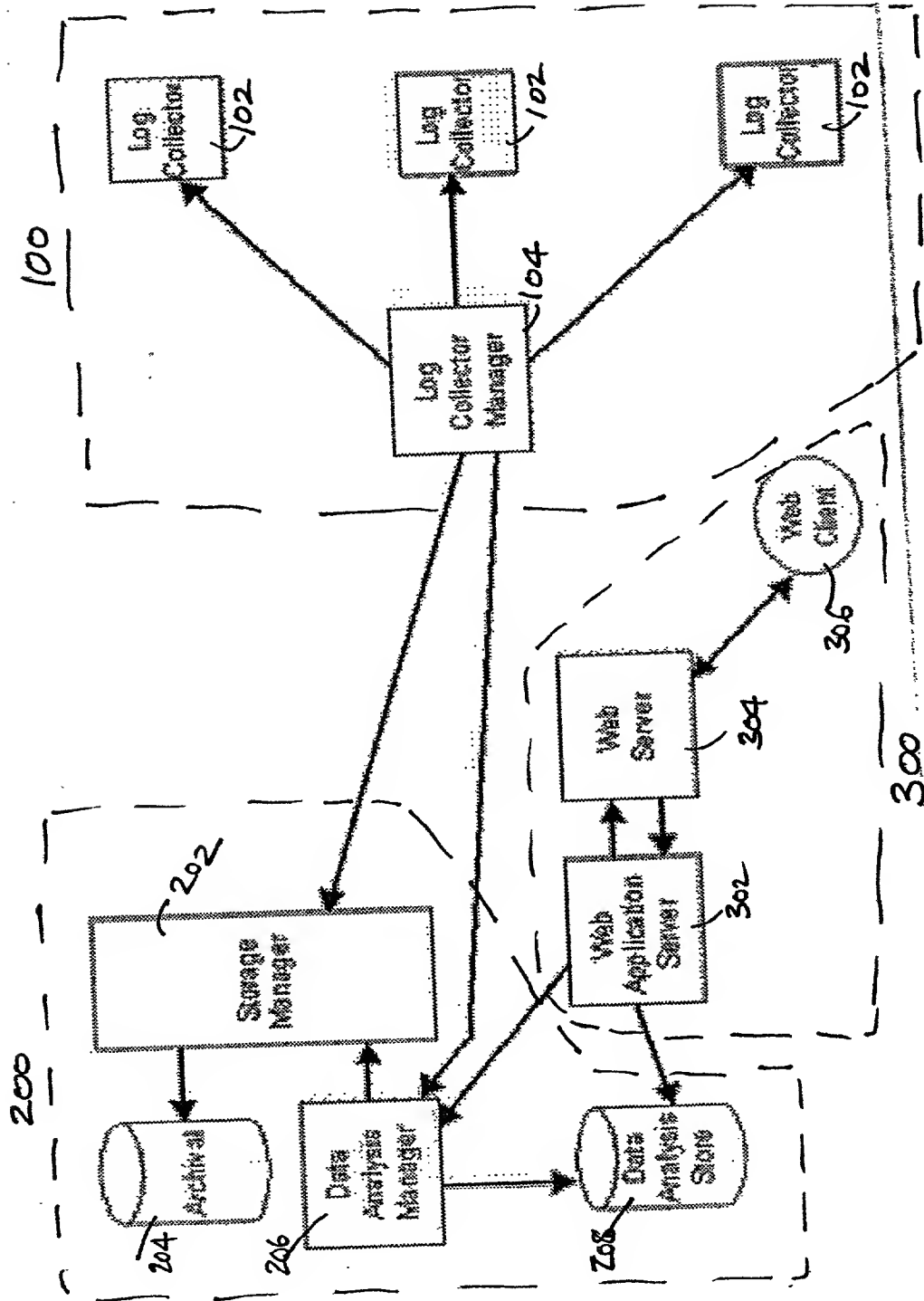



FIGURE 2.



## LOG REPORTING

Login ID:

Password:


FIGURE 3

This is the Admin screen

Although all the tabs appear on this screen, each individual will only get a subset of these tabs based on the status assigned to their screen

Initially none of the tabs are selected

Once a tab has been selected the menu gets replaced with the menu of tabs that have been set up for that particular



Main Results	Configure Filters	Job Status	Logs Archived	Admin
--------------	-------------------	------------	---------------	-------

**MAIN MENU**

Select tab of choice

FIGURE 4

FOUO 14-00000

On a first look  
it seems to be  
the same as the  
one in the first  
part of the book  
but it is not  
the same as the  
one in the first  
part of the book

Metric Results					
Firewall	Gateway Switches	FTP DropBoxes	SPAM	Corporate Security	Main Menu
<p align="center"><b>Main Metric Results Menu</b></p> <p align="center">Select tab of choice</p>					

FIGURE 5.

They is the first  
reaction  
They will appear where  
possibly are indicated  
from the most minute  
The lower world often  
shows the self they  
want to look at  
another than or  
through  
The upper can enter  
the state and present  
information that they  
want to look at  
They could also  
change to remove the  
other present  
of elements available by  
changing the  
different into across  
the eye  
Flame made this the  
QUANTUM BEAM  
only appear if the  
need of seeing the  
element has  
permeated to the 5th  
type thing.  
Any time the state  
changes the date  
necessary, usually  
necessary radio  
beams, they will be  
present to be other  
a state If a month  
before is expected  
they the date would  
only by year and  
month

Metric Results - Firewalls			
Firewalls	Sum of all Firewalls	Used Statistics	Results Main Menu

List of Firewalls

☒ Daily  
☐ Monthly  
☐ Monthly Summary

---

☒ Metrics  
☐ Keyword Results

Enter a date or a date range (format YYYYMMDD)

Single Date:

OR

Range:  to

SUBMIT

FIGURE 6

ॐ नमो भगवते वासुदेवाय  
 श्रीकृष्णाय नमः  
 श्रीगुरुभ्यो नमः  
 श्रीगणेशाय नमः

Metric Results - Firewalls				
Firewalls:	Sum of all Firewalls	Unaid Statistics	Results Main Menu	
RESULTS (Row 1 - 5 of 25):				
Date	Metric1	Metric2	Metric3	Metric4
19990101	4567			
19990102	6543			
19990103	9999			
19990104	4567			
19990105	4567			

PAGES OF RESULTS: 1 2 3 4 5

FIGURE 7.

The page number  
 and date of  
 completion of the  
 work are to be  
 indicated in the  
 margin of the page

[illegible]

FIGURE 8


The month that was selected by the previous window appears on the left side of month or range of months field. The results on the right only appears once the submit button has been pressed.

Any change to the info on the left will clear the results and user must click SUBMIT has been done.

The last page could have a total if target.

If there are more metrics than will appear on the screen, there will be a scroll bar.

This example shows what will be displayed for metrics.



**Metric Results - Firewalls**

Firewalls

Sum of all Firewalls

Userid Statistics

Results Main Menu

**Monthly Summary of Firewalls**

Month or Range of Months

☒ Metrics  
☐ Keyword Results

SUBMIT


**RESULTS (Row 1 - 5 of 15):**

Month	Metric1	Metric2	Metric3	.....
199901	4567			
199902	6543			
199903	9999			
199904	4567			
199905	4567			

PAGES OF RESULTS: 1 2 3

FIGURE 9

Once the user has selected a date, they must then select a firewall and user. The example on the right shows how the information will be displayed if the user chooses all firewalls and all users. The results will show a bar for each user for each date. The names displayed will be a sum for all firewalls.



**Metric Results - Firewalls**

Firewalls

Sum of all Firewalls

Userid Statistics

Results Main Menu

All Firewalls

All Users

Date or Range of Dates

☒ Daily  
☐ Monthly  
☐ Monthly Summary

☒ Metrics  
☐ Keyword Results

SUBMIT

**RESULTS - SUM FOR ALL FIREWALLS (Row 1 - 5 of 25):**


Date	Userid	Metric1	Metric2	.....
19990101	testuser1	4567		
	holkeis	6543		
	sjkfdsl	9999		
	sdjfkldz	4567		
19990102	testuser1	4567		

PAGES OF RESULTS: 1 2 3 4 5

FIGURE 10

Once a regular expression has been added, it cannot be changed because the NAT description and status can.

When adding a new expression, the status is set to ACTIVE



### Configure Filters - Devices

Device List

Search & Count

Search & SUM

Keywords

Configure Main Menu

List of Device Types


List of Logfile Types

SEARCH FOR A PARTICULAR EXPRESSION AND COUNT THE NUMBER OF LINES WHERE THE TEXT WAS FOUND.

STATUS	REGULAR EXPRESSION	TEXT DESCRIPTION
ALL	telnet.*connection for	Number of Telnet Connections
ALL	Bp.*connection for	Number of FTP Connections
ALL	Bp.*file	Number of FTP File Transfers
A		
A		

Save Changes

FIGURE 11



### Job Status - Alarms

Active Severity 1 Alarm

Active Non-Sev 1 Alarm

Acknowledged Alarms

Main Menu

List of Device Types

ALARMXXX - FIREWALL XXXX IS DOWN  
more information about the alarm

ACKNOWLEDGE: ☐

ALARMYYY - FIREWALL YYY NOTICED SOMETHING BAD  
more information about the alarm

ACKNOWLEDGE: ☐

FIGURE 12

FOUO - 1299660

**Logs Archived**

Enter a date or a date range (format YYYYMMDD):

Single Date:

OR

Range:  to

FIGURE 13.

To add a new user, the user must have a valid

The entries in the device type list are taken from the device\_type table.

The entries for the type of access are taken from the access\_type table and are usually DBA, ANALYST.

More functions may be made if the user were able to see different device types. If they were able to see DBA for FIREWALL, security would be made and if they were able to see ANALYST for SPAM, a separate entry would be made.

**Administration**

Userid:

User Name:  Ext:

Device Type:

Type of Access:

FIGURE 14.